# Comment concilier le commerce électronique et la protection de la vie privée

Louveaux, Sophie

*Published in:*
Droit des technologies de l'information - Regards prospectifs - A l'occasion des vingt ans du C.R.I.D.

*Publication date:*
1999

*Document Version*
le PDF de l'éditeur

# COMMENT CONCILIER LE COMMERCE ÉLECTRONIQUE ET LA PROTECTION DE LA VIE PRIVÉE ?

**Sophie LOUVEAUX***

## INTRODUCTION

**1**. Le commerce électronique crée de nombreux risques pour la vie privée. Ces risques ne sont pas uniquement liés au commerce électronique en lui-même, mais également à l'utilisation d'Internet.

La masse d'informations qui circulent sur l'Internet ne fait qu'augmenter : il suffit à cet égard de penser aux 150 millions de personnes qui ont accès à l'Internet à travers le monde et qui peuvent transmettre des données à caractère personnel simplement en cliquant sur le bouton « send » de leur e-mail. L'intrusion dans la vie privée ne fait que grandir quand on pense que cette transmission peut également se faire de manière passive et occulte, notamment par le biais de l'utilisation de « cookies » et d'hyperliens invisibles.

**2.** Internet crée donc des enjeux et des risques pour les données à caractère personnel, qui pourraient remettre en question certains des principes clés de la nouvelle loi belge du 11 décembre 1998[1] transposant la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation des données[2]. La présente contribution a donc pour dessein de montrer comment certains principes fondamentaux de la loi, brièvement rappelés, sont battus en brèche par l'utilisation d'Internet dans le contexte du commerce électronique.

## DONNÉES À CARACTÈRE PERSONNEL

**3.** Il existe plusieurs types de données qui peuvent être collectées lors de l'utilisation d'Internet : les données livrées par la personne concernée elle-même, les données de connexion et les données de navigation. Par

* Assistante au CRID-FUNDP.

1 *M.B.*, 3 février 1999, p. 3049.

2 Adoptée le 24 octobre 1995, *J.O.C.E.*, L 281/31.

ailleurs, toutes ces données peuvent être regroupées, organisées, comparées et recoupées afin de créer des profils d'internautes bien déterminés.

**4.** Très souvent, lorsque la personne concernée désire effectuer une transaction électronique, elle livre elle-même ses données à caractère personnel afin de permettre la réalisation de la transaction (elle donnera son nom et son adresse, par exemple, afin de se faire livrer les biens commandés). Nous nous retrouvons de toute évidence en présence d'une personne identifiée. Mais cela n'est pas toujours le cas. Si la personne navigue sur le Web sans livrer elle-même ses données à caractère personnel, elle laissera néanmoins des traces.

**5.** En effet, lors de la simple connexion à un site, un certain nombre de données sont transmises au site par le programme de navigation (données de connexion), notamment : l'adresse TCP/IP[3], la marque et version du programme de navigation, la marque et version du système d'exploitation, la langue parlée par l'internaute, et les *cookies* éventuels déjà envoyés par le site.

Internet permet d'acheminer tout type de données numériques entre deux machines respectivement identifiées par une adresse TCP/IP, c'est-à-dire l'identité du micro-ordinateur sur le réseau. Il s'agit d'un numéro unique. En pratique, un ordinateur connecté en permanence au réseau aura une adresse TCP/IP fixe, assignée par le gestionnaire de réseau. Un utilisateur occasionnel se connectant par modem recevra, pour la durée de sa connexion, une adresse TCP/IP dynamique, c'est-à-dire différente d'une connexion à l'autre. L'adresse TCP/IP révèle dès lors l'identité de l'ordinateur sur le réseau, mais elle ne révèle pas en elle-même l'identité de l'utilisateur de l'ordinateur. Ceci étant dit, le fournisseur d'accès peut faire le lien entre l'adresse TCP/IP dynamique et l'utilisateur, et le gestionnaire de réseau peut faire ce même lien entre l'adresse TCP/IP fixe et l'utilisateur[4].

**6.** Quant aux données de navigation, lorsque les utilisateurs accèdent à un site, tous leurs faits et gestes sont automatiquement enregistrés : l'analyse du contenu des pages visitées, la fréquence de consultation de ces pages, le temps passé à la consultation et enfin le contenu des achats qu'un consommateur peut faire au cours de sa navigation sur un site de commerce électronique. Tout ceci permet bien évidemment aux sites de rechercher la meilleure organisation de leur site et ce afin de répondre aux attentes des visiteurs.

**7.** À partir de ces différentes données, il devient possible de constituer de vastes bases de données qu'il est relativement aisé de rendre nominatives. Des données à caractère personnel acquises et conservées de

3 « Transmission Control Protocol/Internet Protocol ».

4 Ou en tout cas l'ordinateur possédant le numéro en question (au sein d'une compagnie, par exemple, le fournisseur ne connaît pas précisément l'identité de l'utilisateur de l'ordinateur).

façon cloisonnée demeurent relativement neutres, mais souvent, lorsqu'elles sont associées à d'autres informations, elles peuvent alors devenir personnelles et sensibles. Et c'est ici que les « cookies » ont un rôle primordial à jouer.

Le système de *cookies* permet à un site visité (ou invisiblement hyperlié : une société de 'cybermarketing' infiltrant une bannière publicitaire, par exemple) d'inscrire sur le disque dur de l'utilisateur des informations sur les sites visités et de marquer ces visiteurs en question, et ce généralement à leur insu. Les *cookies* permettent donc de s'affranchir du caractère variant de l'adresse TCP/IP dynamique : si celle-ci change, le *cookie* reste identique de connexion en connexion. À cette marque particulière peut alors être reliée toute une série d'informations relatives au parcours de l'utilisateur sur l'Internet. On est dans un système d'identification stable et durable. C'est donc ici que se trouve le véritable enjeu de la protection des données personnelles, non pas strictement du fait des cookies, mais du fait des traitements qu'ils autorisent entre un ensemble d'informations qui, prises chacune de manière isolée, peut être à juste titre considérée comme relativement neutre.

**8.** La loi belge a tenu compte de cette hypothèse en adoptant une définition très large de la donnée à caractère personnel. Ainsi, est considérée comme donnée à caractère personnel, « toute information concernant une personne physique identifiée ou identifiable »[5]. Selon ce même article « est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».

Par ailleurs, l'exposé des motifs de la loi[6] considère que dès qu'il existe un moyen raisonnable d'identifier la personne concernée, soit dans le chef du responsable du traitement, soit dans le chef d'un tiers, il s'agit d'une donnée à caractère personnel et cela, même s'il n'y a aucune volonté de recherche d'identification de la part du responsable du traitement. Cela permet d'inclure dans le champ de la loi des données tels que le numéro de TCP/IP ou d'autres données de navigation qui permettent au responsable du traitement ou à un tiers d'identifier la personne concernée.

5 L'article 1§1 de la nouvelle loi.

6 Voir Exposé des motifs, *Doc. Parl*., Ch. Repr., Sess. ord. 1997-1998, n° 1586/1, (ci-après exposé des motifs) p.12.

## CHAMP D'APPLICATION TERRITORIALE DE LA LOI BELGE[7]

**9.** Si, *a priori*, la notion de donnée à caractère personnel n'est pas remise en question par Internet, les critères définis dans la loi belge quant à l'application territoriale de la loi posent certaines difficultés.

**10.** La loi belge décrit deux facteurs qui déterminent le champ d'application territorial. Selon le premier facteur, la loi est applicable dès que le traitement « est effectué dans le cadre d'activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge ou en un lieu où la loi belge s'applique en vertu du droit international public »[8]. Imaginons, par exemple, une société dont la maison-mère est en Angleterre, disposant d'une filiale en Belgique, et qui vend des livres en Belgique *via* son site Web, et ce, sans passer par sa filiale belge (le traitement se fait donc en Angleterre), la loi belge ne s'applique pas.

**11.** Le deuxième facteur qui détermine si la loi belge est applicable, concerne les cas où le responsable du traitement n'est pas établi sur le territoire de la Communauté européenne et « recourt à des fins de traitement des données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire belge, autres que ceux qui sont exclusivement utilisés à des fins de transit sur le territoire belge »[9].

**12.** Une première interprétation de cette disposition consiste à appliquer le texte de l'article à la lettre. Dans le contexte de l'Internet, une telle solution mène alors à l'extension de l'application de la loi belge dès qu'un utilisateur étranger collecte des données à caractère personnel à partir d'une base de données ou d'un site Web situé sur le territoire belge. Cela impliquerait que cette personne soit qualifiée de responsable du traitement et doive nommer un représentant établi sur le territoire belge afin de respecter l'ensemble des principes de la loi. Ceci nous semble excessif. De plus, il reste le problème de la localisation de la base de données ou du site Web, dans la mesure où une adresse de site ne correspond pas nécessairement à la localisation géographique du site : http://www.telepathic.com ne nous dit pas où ce site se trouve, ni si en consultant les données à caractère personnel qu'il détient nous devons respecter la loi belge.

---

7 Voir également C. DE TERWANGNE et S. LOUVEAUX, « Data protection and online networks », *The Computer Law and Security Report*, July-August 1997, Vol.13, Issue 4, p. 237.

8 Article 3*bis* , 1° de la nouvelle loi.

9 Article 3*bis*, 2° de la nouvelle loi. D'après l'exposé des motifs, le terme 'moyens' « recouvre tout équipement possible, tels que les ordinateurs, les appareils de télécommunication, les unités d'impression, etc., à l'exclusion, formulée explicitement, des moyens qui sont uniquement utilisés pour le transit des données à caractère personnel par le territoire, tels que les câbles, les routers, *etc*. » (Exposé des motifs, p. 27).

**13**. Une deuxième interprétation, consiste à rechercher la *ratio legis* de ce principe. Celle-ci consiste à éviter que le responsable du traitement cherche délibérément à contourner les lois nationales prises en vertu de la directive en délocalisant son établissement dans un pays tiers, tout en utilisant des moyens situés sur le territoire européen, et ce, sans tomber sous le coup de l'application des articles sur les flux de données vers les pays tiers. Deux catégories de traitements tombent alors dans le champ d'application de l'article 3*bis*, 2° de la loi : le premier vise les traitements portant sur des données à caractère personnel de personnes situées en Belgique effectués par une personne qui a délibérément cherché à contourner la loi en délocalisant son établissement dans un pays tiers, tout en utilisant des moyens situés sur le territoire belge. Le deuxième type vise le cas où le responsable du traitement réalise, par des moyens propres situés sur le territoire belge, un flux de données vers un pays tiers où il traite les données[10] (on pense aux cas des *cookies* placées sur le disque dur d'un belge lors de la consultation d'un site Web). Le critère principal qui détermine l'application de la loi à des responsables situés en dehors du territoire de la Belgique n'est donc pas uniquement limité au recours à des moyens situés sur le territoire de la Belgique. Une analyse plus fouillée doit être effectuée afin de déterminer si le responsable du traitement s'est délocalisé de manière à éviter l'application de la loi belge. Cette analyse est cependant difficilement réalisable dans le contexte d'Internet où l'identité des responsables de traitement n'est pas facile à déterminer.

## PRINCIPES DE PROTECTION DES DONNÉES

**14**. Quant aux principes de protection des données tels que préconisés par la loi belge, il semble qu'Internet remette en question l'application de certains d'entre eux, suscitant des préoccupations quant à la protection de données à caractère personnel.

10 Les articles de la nouvelle loi belge relatifs aux transferts de données à caractère personnel vers des pays tiers non-membres de l'Union européenne ne s'appliqueraient pas dans ce cas, étant donné qu'ils ne s'appliquent que lorsque le responsable du traitement qui effectue le transfert est localisé en Belgique. Voir *infra* à propos des flux de données en dehors de la Communauté européenne.

## LE PRINCIPE DE FINALITÉ LÉGITIME

**15.** Selon la loi belge, les données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités[11].

**16**. En ce qui concerne l'obligation de ne pas traiter les données ultérieurement de manière incompatible avec les finalités pour lesquelles les données ont été collectées, la loi précise que la compatibilité doit tenir compte de tous les facteurs pertinents, notamment « des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables ». Le recours aux attentes de l'intéressé se situe dans l'idée de transparence, afin d'éviter que la personne méconnaisse une utilisation ultérieure des données la concernant. En matière de commerce électronique, par exemple, en ce qui concerne la vente de produits *via* Internet, les consommateurs qui transmettent leurs données à des fins d'achats sur le site considèrent que les données ainsi transmises ne seront traitées qu'à des fins en lien direct avec le service offert (envoi de la marchandise, facturation du service …). Toute autre finalité qui n'entre pas dans le champ de l'attente raisonnable de l'intéressé devra lui être signalée et sera considérée comme une nouvelle finalité à part entière.

**17.** Les fournisseurs d'accès disposent, de par leur fonction, de toute l'information générée par les connexions et la navigation de l'utilisateur ainsi que les coordonnées personnelles nécessaires à la facturation du service fourni. Tant que les fournisseurs d'accès se contentent de rester dans leur fonction de transporteur des messages et respectent un certain nombre de principes, comme celui de l'information préalable ou de la qualité des données[12], ils restent dans le cadre du principe de finalité légitime et compatible. Toutefois, s'ils s'avisaient d'élargir leur service et d'exploiter les données qu'ils détiennent ou de les commercialiser, cela changerait considérablement la nature du service. Or la tentation est grande et certains fournisseurs d'accès se sont d'ailleurs déjà lancés dans des offres de fourniture d'accès gratuit avec, en contrepartie pour l'utilisateur, de renseigner très précisément sur son profil. Il y a donc un glissement en ce qui concerne la finalité poursuivie par le fournisseur d'accès, glissement qui peut inquiéter quant aux réelles garanties de protection des données à caractère personnel pour l'internaute.

11 Voir article 4 de la nouvelle loi.

12 Voir *infra*.

## FONDEMENT DU TRAITEMENT : LE CONSENTEMENT DE LA PERSONNE CONCERNÉE

**18.** La loi prévoit que les traitements ne peuvent être poursuivis que dans l'un des cas visés par son article 5 et, notamment, si la personne concernée a donné indubitablement son consentement. Un consommateur qui introduit ses propres données afin d'effectuer un achat sur Internet sera présumé comme ayant donné son consentement au traitement de ses données pour les finalités qui lui ont été déclarées. Toutefois, l'hypothèse d'un consentement donné par Internet lors d'une transaction électronique pose certaines questions.

**19.** Selon la loi, le consentement écrit n'est pas requis sauf pour le traitement des données considérées comme des données sensibles[13]. Cela implique que le consentement puisse être donné de manière électronique[14]. Toutefois, sauf en cas de signature digitale, la preuve d'un consentement à l'utilisation de ses données par le simple « cliquage » d'une icône n'ira pas sans poser certaines difficultés.

**20.** Le consentement doit par ailleurs être : « une manifestation de volonté, libre, spécifique, et informée »[15].

**21**. Une manifestation de volonté *libre* implique qu'il ne devrait y avoir aucune pression sur l'individu afin d'obtenir son consentement. Le refus d'acceptation du consommateur lors de la demande de données à caractère personnel par un site ne devrait pas, en principe, être retenu contre lui. Cela est également vrai pour l'utilisation de *cookies* : le refus d'un *cookie* ne devrait théoriquement pas porter préjudice à l'accès au site par le consommateur ni le service fourni par ce site. Toutefois, dans la réalité du commerce électronique il en va bien autrement. La commercialisation d'informations que les sites ou les fournisseurs d'accès détiennent sur leurs clients est, en effet, l'une de leurs sources de revenus principales. Lorsqu'une personne désirant effectuer des achats sur Internet accède à un site qui lui réclame des données à caractère personnel, par exemple, le refus par la personne concernée de livrer ses données implique le refus de la part du site en question de lui permettre de bénéficier des services offerts. Si l'ensemble des sites de commerce électronique lui refusent le service pour ce même motif, la personne désirant effectuer une transaction par Internet, n'aura plus réellement le libre choix de refuser ses données. D'autre part,

13 Les données sensibles sont les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la vie sexuelle, à la santé et à des litiges soumis aux cours et tribunaux. Voir à ce sujet les articles 6, 7 et 8 de la nouvelle loi.

14 Cette possibilité a d'ailleurs été envisagée par la loi allemande : voir l'article 2, §3, 7 de la loi allemande « Informations - und Kommunikationsdienste - Gesetz - IuKDG » du 1er août 1997 (publiée au *Bundesgesetzblatt* du 28 juillet 1997).

15 Voir la définition donnée à l'article 1er, §8 de la loi.

un consommateur qui refuserait de livrer des données à caractère personnel à un fournisseur d'accès se verrait purement et simplement refuser l'accès à Internet.

**22**. Toujours selon la définition légale, le consentement doit être *spécifique* : il doit porter sur des traitements précisément définis et non sur des objets généraux. Toute modification de la finalité qui n'est pas considérée comme compatible avec la finalité déclarée requiert donc un nouveau consentement.

**23.** Enfin, le consentement doit être *informé* : cela suggère que les vendeurs sur Internet informent les utilisateurs des risques potentiels de l'Internet vis-à-vis de la protection de leurs données à caractère personnel. Cela permet au consommateur de mettre en balance ces risques avec les bénéfices attendus. L'avantage d'Internet est qu'il permet justement d'assurer une bonne information en temps réel à la personne concernée.

**24.** De plus, l'interactivité qui caractérise les réseaux tels qu'Internet offre certaines facilités en ce qui concerne le consentement de la personne concernée. Plutôt qu'un consentement donné une fois pour toutes au début d'une série d'opérations, l'interactivité permet de moduler le consentement. Un message peut apparaître sur l'écran annonçant que si le consommateur veut poursuivre la transaction, il doit consentir à livrer telle ou telle information. Il peut accepter une partie de l'opération mais refuser de donner davantage de données à caractère personnel pour une autre partie de la transaction. De plus, les mécanismes de *'opt-in'* ou de *'opt-out'* prennent une dimension immédiate et effective à travers l'interactivité : le consommateur peut cocher les cases correspondant à des utilisations secondaires de ses données.

## LES PRINCIPES DE CONFORMITÉ ET DE QUALITÉ DES DONNÉES

**25.** Selon la loi[16], les données à caractère personnel doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ». Cette exigence assure qu'il existe un lien suffisant entre les données et la finalité poursuivie.

**26.** De nombreux sites demandent aux visiteurs réguliers, et parfois même également aux surfeurs occasionnels, de remplir un formulaire d'inscription avant de pouvoir accéder au site. Il est essentiel que les données à caractère personnel qui sont demandées soient pertinentes. L'adresse e-mail de l'utilisateur peut être nécessaire afin de fournir le

16 Article 4, §1er, 3° de la loi.

service, alors que des informations sur l'âge de la personne, son statut civil ou ses revenus peuvent être considérées comme des données excessives ou non pertinentes. Ce type de données peut aider l'opérateur du site à constituer des profils de visiteurs, soit pour des fins propres, soit pour le compte d'un tiers, mais si ces profils ne cadrent pas dans les finalités déclarées, un tel traitement des données serait incompatible avec les finalités déclarées.

**27.** Les données doivent également être « exactes et si nécessaires mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées »[17]. Il s'agit donc d'une obligation de diligence du responsable du traitement qui doit tout faire pour que les données soient exactes. La configuration d'Internet ne facilite pas le respect de cette obligation. Il s'agit d'un réseau de données variables en qualité et en exactitude. Ainsi, comme nous le verrons ci-dessous, l'utilisation d'Internet peut entraîner la création de profils virtuels qui ne correspondent aucunement à la réalité.

**28.** La participation de la personne concernée à la collecte des données et la possibilité effective d'un droit de rectification[18] sont des mesures qui peuvent contribuer à la qualité des données.

**29**. Les données doivent être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement »[19]. Ainsi, des données collectées auprès d'un client afin de fournir des biens et services ne devraient pas être gardées au-delà de la période nécessaire pour cette finalité, sauf consentement exprès de la personne concernée.

## LES TRANSFERTS DE DONNÉES VERS DES PAYS TIERS

**30.** Le commerce électronique peut et va certainement générer des transferts de données vers des pays tiers. Quels sont les principes établis par la loi belge à cet égard et comment s'appliquent-ils dans un contexte de transaction électronique ?

**31**. En principe, selon l'article 21 de la loi, « le transfert de données à caractère personnel faisant l'objet d'un traitement après leur transfert vers un pays non-membre de la Communauté européenne, ne peut avoir lieu que

17 Article 4, §1er, 4° de la loi.

18 Voir les articles 9 et 12 de la loi.

19 Article 4, §1er, 5° de la loi.

si le pays en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions de la présente loi et de ses arrêtés d'exécution »[20]. La loi prévoit toutefois, en son article 22, un certain nombre d'exceptions, notamment si la personne concernée a indubitablement donné son consentement au transfert, ou si le transfert est nécessaire à l'exécution d'un contrat.

**32.** En dehors des exceptions prévues, l'évaluation du caractère adéquat de la protection doit se faire avant la transmission des données. Cela ne va pas sans poser certains problèmes dans le contexte du commerce électronique. À cet égard, nous devons distinguer deux types de transferts : les transferts actifs de données, qui sont des transferts initiés par la personne concernée ou en tout cas avec son accord ; et les transferts passifs, qui eux se font à l'insu de la personne concernée.

**33.** En ce qui concerne les transferts actifs, en principe la personne concernée consent, au moins implicitement, au transfert de ses données vers un pays tiers[21]. Cependant, il convient de faire remarquer que les règles émises dans la loi sont basées sur une présomption que les transferts de données suivent toujours un itinéraire précis et direct, ce qui n'est pas le cas des flux sur l'Internet. En effet les messages, ou l'ensemble des données transférées, sont envoyés *via* le *routing* le plus rapide au moment de la transmission. Tout obstacle technique lors de la communication engendre un éclatement du message en 'paquets' qui suivront un itinéraire différent à travers le réseau pour arriver en entier chez le destinataire. Les pays destinataires dans le cadre du transfert des données sont donc imprévisibles, et une évaluation *a priori* de la protection offerte semble donc difficilement praticable. D'autre part, puisqu'il est possible d'accéder à un site Internet de partout à travers le monde, il semble difficile pour le responsable du site en question de limiter l'accès seulement aux pays offrant une protection adéquate. Quand bien même cela serait le cas, comment le responsable du site pourrait-il être sûr de la localisation physique de la personne accédant au site ?

**34**. Quant aux flux passifs, à savoir les flux de données à caractère personnel qui sont effectués à l'insu de la personne concernée, nous distinguons l'hypothèse des *cookies* des autres traces électroniques laissées lors de la visite d'un site[22]. À propos des *cookies*, puisqu'ils permettent une collecte discrète de données à l'insu de la personne concernée, il nous semble difficile de qualifier la personne en question d'expéditeur des données ni même de parler d'un transfert de données. Il s'agit plutôt en

20 Il semblerait que l'appréciation du caractère adéquat revient au responsable de traitement ; toutefois, selon l'alinéa 2 de l'article 21 de la loi, il est loisible au Roi, « après avis de la Commission de protection de la vie privée », de déterminer « pour quelles catégories de traitements et dans quelles circonstances la transmission n'est pas autorisée ».

21 Nous tombons alors dans une des exceptions visées à l'article 22 de la loi.

22 Voir *supra* : Données à caractère personnel.

effet d'une collecte de données, et puisque la personne responsable de la collecte est située en dehors de la Communauté européenne mais recourt à des moyens situés sur le territoire d'un État membre, c'est l'article 3*bis* plutôt que les articles 21 et 22 de la loi qui devrait s'appliquer[23].

**35**. Quant à la deuxième hypothèse des traces laissées lors de la visite d'un site à l'insu de la personne concernée, il ne peut s'agir d'un transfert de données à caractère personnel puisque la personne concernée n'effectue pas un flux conscient de données. L'article 3 bis ne s'appliquera pas non plus étant donné que le responsable peut prétendre ne pas collecter les données en ayant recours à des moyens situés sur le territoire d'un État membre : il ne fait que collecter les données lors de la visite de la personne sur son propre site. La loi laisse donc la personne concernée sans protection quant aux traces qu'elle peut laisser. Elle doit être informée de ce danger.

## CONCLUSION : ENJEUX ET RISQUES

**36.** Au regard de cette protection légale, quels sont les enjeux de l'utilisation d'Internet dans le contexte du commerce électronique pour la protection des données et la vie privée des utilisateurs ?

**37**. Il ne semble pas, selon nous, que le réel enjeu réside dans la possibilité d'envois publicitaires non sollicités à partir des profils comportementaux obtenus par le biais d'Internet (*spamming*). En effet, ces sollicitations commerciales constituent plutôt une gêne qu'une véritable intrusion dans la vie privée des personnes. Cela étant, il faut tout de même signaler que la directive européenne 97/66/CE « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications »[24], interdit l'utilisation d'automates d'appels téléphoniques ou l'usage de fax, à des fins de prospection directe sans le consentement préalable de la personne concernée. Ceci semble indiquer qu'il existe néanmoins une certaine préoccupation quant à la protection de la vie privée dans le cadre de la prospection commerciale.

**38**. Le réel danger, selon nous, réside plutôt dans la possibilité de constitution de profils comportementaux et d'identités virtuelles entraînant la perte de contrôle de chacun de sa propre image. Le risque est que les responsables de sites ou les tiers auxquels les données sont cédées, déduisent d'un comportement ou d'une série d'achats, une personnalité qui ne correspond aucunement à la réalité. En effet, un consommateur peut acheter des biens pour le compte d'un tiers ou visiter des sites qui ne correspondent pas à ses centres d'intérêts réels. Plus grave encore est la

23 Voir *supra* : Champ d'application territoriale.

24 *J.O.C.E.*, 30 janvier 1998, L 24/1.

perte du pouvoir de gestion de sa propre image. Un internaute donne telle information, dans tel contexte et pour telle finalité (par exemple, il donne telle donnée parce qu'elle est nécessaire à la réalisation d'une transaction qu'il a voulue), mais ce qu'il ignore c'est le croisement qui sera fait de cette information avec d'autres informations acquises de tiers ou acquises de manière occulte.

**39.** À cet égard, la nouvelle loi belge relative à la protection des données dispense le responsable du traitement de fournir aux personnes concernées une série d'informations visant à assurer la transparence du traitement, lorsque « l'information se révèle impossible ou implique des efforts disproportionnés »[25]. Il appartient au Roi de déterminer, par arrêté royal et après avis de la Commission de la vie privée, les conditions d'application de cette disposition. Il est à espérer que cette disposition ne pourra pas s'appliquer, dans le contexte d'Internet, pour les personnes ayant obtenu des données par le biais du réseau et qui, de par le manque de lien direct entre elles et la personne concernée, ont des difficultés à fournir les informations nécessaires à la personne concernée. En effet, si le responsable est néanmoins tenu de respecter les autres dispositions prévues dans la loi, la personne concernée perd une large partie du contrôle sur ses propres données : comment, par exemple, peut-elle exercer ses droits d'accès et de rectification si elle n'est pas informée quant aux personnes possédant ses données ?

**40**. Dès lors, si la protection offerte par la loi belge présente certaines faiblesses dans un contexte de transactions électroniques, il nous semble que la personne concernée doit avant tout être pleinement informée des risques et enjeux de l'Internet. Seule une parfaite transparence vis-à-vis de l'internaute permettra à celui-ci de mesurer les risques pour ses données lorsqu'il procède à de telles transactions.

25 Voir article 9, §2, alinéa 2 de la loi.